Banc Ceannais na hÉireann
Central Bank of Ireland
Eurosystem

Speech

Operational Risk Assessments – Perspectives from the Central Bank of Ireland (‘CBI’)

Speech given by

Lisa O’Mahony, Head of Function, On-site Inspections, Insurance Supervision, Central Bank of Ireland

Society of Actuaries in Ireland (SAI), Risk Management Perspectives Conference, Dublin, Ireland

25 October 2017

I am grateful to Lenka Marsikova, Susan Forristal and Fiona Brosnan for their contributions to this speech.

Introduction

Good morning, it is a pleasure to join everyone here today, and thank you to the Society of Actuaries for inviting me to speak at your Risk Management Perspectives Conference.

As mentioned, my name is Lisa O'Mahony and I am Head of Function for the On-site Inspections team in the Central Banks' Insurance Supervision Directorate. I joined the Central Bank over five years ago. Over that time, I have led supervision teams across the life and non-life sectors, and supervised both domestic companies and companies within international groups. Then almost two years ago, I established the On-site Inspections Function, and we provide support across the various insurance sectors.

As well as performing a number of inspections in other areas, a key priority for the on-site team was to perform a number of operational risk inspections over the past 18 months. We performed these in reference to the regulatory requirements of Solvency II and the Corporate Governance Code. We also referred to best practice guidance.

Based on this work we are in a position to benchmark companies against their peers. We compare companies across their governance frameworks, and key processes for identifying, managing and reporting of operational risk.

I am cognisant of the huge efforts made by the industry over the past number of years in preparation for, and implementation of Solvency II. I am mindful that it can be difficult to take the theory of the phrase 'embed risk management', and make it real in practice. Given that our inspections are, evidence based; this is something that we ourselves had to think long and hard about. What would evidence of an embedded risk management framework and an effective risk culture look like?

Through our inspections, we have seen a variety of approaches and you will have seen these outlined in our Dear 'CRO' letter to industry. Following that, I was invited here today share some of our insights and out some colour on our experiences.

Agenda

I have chosen to start by looking at the appropriateness of capital for operational risk, then discuss some ways to make risk identification and reporting of operational risk more effective in practice, and finally finish on some thoughts on how to shape the risk culture.

But, first why does operational risk matter?

There are many answers to that question. Unfortunately, I only have a half hour to speak and I will not be able to go through every source of operational risk today, however, there are two dominating factors.

Firstly, operational risk incidents can have financial, reputational and operational impacts. Secondly, it is a key risk under Solvency II that could be explored more by companies, in terms the Own Solvency Needs assessment.

As you know, unlike the financial risks of insurance, operational risk is slightly more difficult to identify and manage in practice, and can often be underestimated. Exposure to operational risk can originate from the external environment, or can emerge internally.

Externally a company can be exposed to one off events such as Cyber-attacks, failure of third party outsource providers or threats to the physical assets. A company may also be exposed to operational risk through one off business transactions, such acquisitions of other companies or back books of business.

In addition, internally operational risk can emerge from almost any part of the business. Often these 'slow burner' risks quickly catch a company off guard when they erupt. These may also be what we refer to as boundary events. That is, something, which has its roots in poor operational risk management, can quickly manifest itself into another risk, such as market or capital risk.

The majority of companies that we supervise, apply the standard formula. As a result, the capital amount included in the Solvency Capital Requirement (SCR) for operational risk is based on a function of size. Many people have argued that this is a crude method of calculating this number. However, there is also a requirement under Solvency II for companies to evidence the appropriateness of the standard formula for their company. This can be achieved through the Own Solvency Needs Assessment process.

Operational Risk and the Solvency Capital Requirement (SCR)

I have prepared some numbers here based on annual returns data. As you can see, the capital allocated to operational risk is on average 7% of the SCR. Only a handful of companies have stated operational risk as being 20%+.

Does this feel right? Given the number of factors discussed earlier that could be a source of operational risk events. How can you actually provide evidence that the amount of capital allocated to operational risk in the SCR is appropriate for your company?

I know that people will argue that operational risk is not about a capital number. That having a credible contingency plan, or strong internal controls, rather than a large capital buffer in place, would be more meaningful methods of counteracting operational risk events.

I agree, from the perspective that companies should not take false comfort from 'a' number. To mitigate against operational risk, there needs to be continuous, on-going risk identification and management, it cannot be neatly boxed off with a percentage, number or formula.

However, what I would say is. Based on what we have seen date, there is room for improvement, for companies to work through the thought process of, identifying operational risk exposures in the first instance, and then working through the options of how to mitigate that risk, or establishing what an appropriate amount of capital is to hold against it. In my mind, the first step is risk identification is core.

Risk Identification

What have we seen in the Risk Identification space?

There needs to be a multi-faceted approach to risk identification. Useful tools are scenario analysis, a sound Risk and Control Self-Assessment process and capturing of actual losses.

Although, we have seen some positive developments, with companies discussing how to identify and quantify potential operational risk exposures. Operational Risk Scenarios included in the Own Risk and Solvency Assessment (ORSA) require further development, and in some cases do not exist at all. Common issues are:

- Companies which are subsidiaries in groups, failing to apply a local perspective to the scenarios, and a lack of reflection on actual entity experience;
- Relying on qualitative scenarios for operational risk with little quantification of potential impacts. For example, have seen companies suffer cyber-attacks, which led to, opportunity costs for down time, and significant remediation costs, which had a clear monetary impact. However, these was not quantified in monetary terms, and was not included as a scenario in the ORSA thereafter;
- We have seen a lack of consideration of potential exposures to loss of services from third party outsource providers.
- Indeed, we have also seen in some cases, companies did not even include a Business Continuity or Disaster Recovery scenario for their own operations.

Generally, there is improvement required.

In addition, scenarios, when they are in place, are typically used to identify external or one off threats. However, we have seen that scenario analysis can also be a very useful tool in each of the business units in the front line, to identify ‘creeping’ or ‘slow burner’ plausible operational risk events. Using scenarios in the business units can lead to a better blend of potential exposures from both the external and internal operating environment.

Another very useful tool, which we have seen for identifying operational risk in the day-to-day processes of companies, is the Risk and Control Self-Assessment Process, the ‘RCSA’. This will position a company to create a risk register for each part of the business. These can then be combined to analyse the full universe of operational risks across the company, at an aggregate level.

However, this process should deliver on both elements of its name – Risk and Controls. Where we have seen companies fall down on this, is the RISK element of this process. Sometimes we have seen risk functions are often very busy testing controls, to satisfy multiple control frameworks that have evolved over time. In this situation, we have seen that companies sometimes fail to take a step back, to think about actual RISK identification. What we would say is to take the RCSA back to basics, ensure you ask, what are the risks?, before launching into a complex programme of control attestation.

Useful aides as part of the RCSA process, can be the use of ‘Blank page’ assessments, discussions on emerging risk, and meetings to discuss ‘boundary losses’. Getting some of the people across the business into a room to identify risks they may not have previously thought of, and potential interdependencies and hot spots where ‘boundary losses’ could emerge.

While scenario analysis and the RCSA process allows a company to identify potential operational losses, capturing actual loss events and near misses allows a company to identify actual operational losses. The reporting of such events can be a valuable source of information, if analysed appropriately for trends and patterns by the risk function. This can sometimes identify systemic control weaknesses.

A challenge to this is that companies generally have a brief history of such losses, and lack sufficient data to provide meaningful and reliable analysis. However, we would encourage the continued development of internal data repositories of operational risk losses and events, and analysis of the same. This will improve how companies identify and manage operational risk exposures for the future.

All three of these methods combined will provide a clearer picture as to what your operational risk exposures may be. In turn, this may lead to better mitigation of those risks. It should also generate a more reliable and quantifiable Own Solvency Needs assessment.

Risk Monitoring and Reporting

It is impossible for a company to eliminate operational risk. Timely and adequate, reporting of these risks will allow a company to be more pro-active and avoid a cycle of firefighting.

In this area, some good practices we have seen include the establishment of a dedicated operational risk committee at the executive level. This ensures a focused, timely conversation and reporting on operational risk matters. This also ensures that operational risk gets sufficient 'air time'. This can enable a firm to quickly respond to changes in the business, the market and emerging risks.

We have also seen that risk managers can find it a challenge to aggregate risk information. Given that, there are often large suites of reporting. It can be difficult to convey key messages, which allows a committee to focus on the issues which are 'heating up'.

We have seen <u>three methods</u> in practice that can help to focus this discussion.

Firstly, monitoring against Risk Appetite. This should be supported by a regular dashboard showing actual operational risk exposures, compared to the expressed appetite. This should include an appetite, for both qualitative and quantitative measures and one off significant events and cumulative lower value type events for operational risks. Risk appetite, should be supported with tolerance thresholds and hard limits that will trigger actions.

Secondly, Key Risk Indicators (KRIs). A key challenge we saw for companies was the interpretation of the 'seriousness' of operational risk events. In practice, what may seem like a serious operational risk event to one person may go unreported by another, if left to personal judgement. We have observed that creating a risk taxonomy or dictionary, can be helpful to address this challenge and create some consistency across business units.

Another issue has been how to <u>aggregate risk</u> indicators. Defining criteria to identify which risks are <u>key,</u> helps to address this challenge.

And thirdly escalation procedures: when these are clearly defined, this can help to avoid risks being omitted, or fading into the background due to over reporting. This requires a company to define thresholds when an event is material enough to be escalated for discussion, either internally or externally.

Risk Culture

Finally, risk culture. The people in your organisation, the decisions that they make, and how they act and behave is the glue that will hold your organisation together, or not. Because operational risk can be 'anywhere' and 'everywhere' in the business, the risk culture is more important than ever, and will be a determining factor in your success or failure, in embedding operational risk management practices.

However, there are multiple layers to risk culture. No one tangible object, action or behaviour defines a risk culture, and there is no silver bullet to shape and embed it. However, there are multiple indicators at the various levels of the organisation. Taking each of those layers:

What are some of the indicators of culture 'at the top'?

Under Solvency II there are increased responsibilities for the board in the area of risk management, including operational risk. Board members are required to take a more active role in the oversight of risk management and Solvency II has been somewhat of a step change in this regard. I would break this into three categories:

Firstly, the *composition of the board* and their ability to steer the operational risk agenda. Good practice observed was a mix of expertise, experience and skills in relation to areas of Operational risk. We have found that where this exists there has been more evidence of challenge, by the board, of the senior management team. One example would be a clear understanding of IT issues.

Secondly, how does the board *discuss operational risk at a strategic level*? We have seen that there is often a weak link between the business strategy, the risk appetite statement, and the scenarios in the ORSA, for operational risk. In practice, it is questionable if the board and senior management team refer to these, when making strategic decisions. Such practices can send a negative message to the business.

Thirdly how have the board sought comfort over what happens on the ground in practice? Have they looked for evidence of the operational risk management framework being effective day to day? From our inspections it is clear, where boards have requested independent parties, such as internal audit or external third parties, to perform end-to-end reviews of the operational risk management framework, the company has benefited from this. Such an audit will give a level of assurance to the board that the frameworks in place are designed appropriately and operating as intended.

This will also indicate the level of ownership and accountability a board exhibits for its risk management framework. Monitoring and discussion of operational risk by the board and risk committee set the tone for the culture. This signals that operational risk is taken seriously, and sends a message that questions will be asked about where the operational risk exposures are, how well they are being managed and could some of them be avoided for the future? This will help embed the ethos that 'operational risk matters'.

What are some of the indicators of culture 'in the middle' layer?

The onus for setting the tone for 'risk culture' also rests with the senior and middle management teams. The Chief Risk Officer and the risk function has an important role in this. However, they need the support and buy in of the other members of the executive management team for this to take traction with the business. Some indicators of culture in the middle layer can be;

- Is an RCSA process conducted, is there evidence that the risk function engaged with the front line business units and not only facilitated this process but challenged the business on their assessments?
- Is there a culture of learning from mistakes and 'after action' reviews? Does the risk function conduct root cause analysis with the business?

Taking this approach is a good indicator of the risk culture. This is proactive risk management and may help avoid mistakes in the future. Sometimes it is more about what people learn from an event or the failure, rather than the incident itself.

And what are some of the indicators of culture 'in the front line'?

Although many companies have come to grips with the design of what should be in an operational risk management framework, the real challenge is in embedding this in the business. From our experience on the inspections, something that has been proven to support this is clarity of roles and responsibilities. These need to be well documented, and clearly communicated.

When on inspection we have often come across the expression that 'risk management is everyone's responsibility'. We agree with this ethos, and it is very positive to see companies working to build risk awareness into everything that people do, throughout the business.

However, to underpin this, there needs to be clarity over who has ultimate responsibility. Unless people are clear on this, things can fall between the cracks. When people are clear on their own role and responsibilities, there is accountability and it is much more likely that people will pay attention. As a result, the framework will be more effective in practice.

Other indicators of risk culture day to day, were the attitudes towards loss events, policies and procedures, performance management and training.

Firstly, ask yourself what is the attitude towards reporting losses, errors and events in your company? Do people report 'near misses? Is this encouraged? Has the risk function and the front line management been able to create a 'no blame' culture, where it is encouraged to report near misses, without reprimand? The appointment of 'risk and error champions' in the business or the 'first line' can be an effective mechanism to achieve reinforcement of the 'risk' message 'on the ground'.

Secondly, are people clear on what to report, when and how? Such lack of clarity can lead to, incidents not being recognised, or if they are recognised that they are not being reported. Training to increase risk awareness so that people will recognise emerging and actual operational risks incidents, as well as clarity on how to report an incident if it occurs, is important.

Finally, of course the reward and compensation system of a company are key drivers behind the culture. After all, 'what is rewarded is perceived as what matters'. It is often helpful to have clear objectives and accountabilities in relation to risk management included in performance conversations. Finding ways to incorporate the risk culture you desire into the reward programme of your company is important.

Final

This brings me towards the end of today's session. In summary, ***What am I saying?***

Overall, from our inspections, we have found that there is no one size fits all, and the framework chosen by each company will depend on the complexity and risk profile of each entity. As an industry, some good progress has been made in the area of operational risk management over the last few years. However, some companies are further along that journey than others are. This has been partly a consequence of prioritising financial and insurance risks ahead of operational risk, but it has also been a challenge to grapple with operational risk.

I hope that you have taken away some ideas today on how to tackle some of the challenging aspects of operational risk management that you are experiencing. However, if I would like you to walk away with three key messages today, I would like them to be:

- Firstly, do not take false comfort from the capital number in the SCR. Scenario and stress analysis are your friend when it comes to operational risk and in assessing your Own Solvency Needs;
- Secondly, remember; always refer back to basics, what are the risks? It may sound obvious, but the rest is just white noise if you have not identified the risks appropriately, and
- Finally, what is the mind-set and the attitude of your people? The Risk Culture. Do people understand what operational risk is? Being proactive in your risk management, repeating the message again and again, and having the right behaviours reinforced through training and day-to-day management will help embed an effective risk culture.

While it is difficult to quantify the reward from the time and resources invested in the management of operational risk, the cost of not doing so may be far greater. Therefore, I encourage you all to continue in your endeavours across all of the areas highlighted today.

Thank you for your time, and once again thank you to the society for inviting me to speak. I hope you enjoy the rest of the conference. I am happy to take some questions now, or I will also be here for the rest of the day if you would like to discuss anything one to one.